Multi-Function Device (MFD)and Printer Checklist for Sharing Peripherals Across the Network Security Technical Implementation Guide Version 1 Release 1.2

14 April 2006

Developed by DISA for the DOD

Database Reference Number: ______________________________ CAT I: _____

Database entered by: _________________ Date: _____________ CAT II: _____

Technical Q/A by: ____________________Date: _____________ CAT III: _____

Final Q/A by: _______________________ Date: _____________ CAT IV: _____

Total: _____

UNCLASSIFIED UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Enclave Reviewer				**Phone**	
Previous SRR	Y N	**Date of Previous SRR**		**S01 Available**	Y N
Number of Current Open Findings					

Site Name	
Address	
Phone	

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				

Summary of Changes

14 April 2006 – Added VMS 6.0 review procedures.
14 April 2006 – Added VMS 6.0 Vulnerability Key to each checklist item.

VMS 6.0 SPAN MFD Review Procedures

The following is an outline of the process for performing a SPAN MFD review and entering the results using VMS 6.0.

1. Ensure that asset is registered in VMS under the correct organization. The asset will have the posture of Computing → Network → Data Network → Network Peripherals → MFD. If the asset has an identifiable operating system the posture will also include the appropriate OS.
2. If the asset is registered skip to Step 4 otherwise you must register the asset. You will find the appropriate selection criteria by selecting Asset Finding Maint → Assets/Findings → By Location → your location → Computing and then click on the file icon to create the asset.
3. On the General tab fill out the Host Name and appropriate values for the other fields on this tab.
4. Determine the enclave that the asset is within.
5. If the asset is in the correct enclave, skip to step 9.
6. Enter the enclave on the Systems/Enclaves tab of the asset creation / or update screen.
7. For registered enclaves, choose the enclave.
8. If the enclave is not present, contact your team lead or your IAM and report that the enclave is not present.

   NOTE: Every effort should be made when registering or updating an asset to include the asset within an enclave.
9. Since at this time there is no scripted review process that automatically generates an import file, only the fields required by VMS need to be filled in unless there are other elements in the asset posture that require specific fields for their scripts. Any additional fields may be filed in for documentation purposes. The more documentation the better for identifying the system correctly.
10. Print the Checklist and perform a manual review for the MFD component.
11. Manually key results into VMS.
    Reviewers: By navigating to the pertinent visit, selecting the asset, and expanding the appropriate element for this review. If the asset is not found in the visit, contact your Team Lead and have them enter the asset into the visit.
    Systems Administrators: by navigating to the your location, selecting the asset and expanding the appropriate element for review.
    The appropriate element will be MFD.
12. Process any additional reviews required by additional elements within the asset posture.

MFD01.001 CAT: **2** MFD Protocol TCP/IP

8500.2 IA Control:	DCPP-1	Category:	14.4 - Unneeded Ports, Protocols, Hardware, and Services
VMS Vul Key:	V0006777		

Vulnerability A network protocol other than TCP/IP is enabled on a MFD or printer.

Vulnerability Discussion: The greater the number of protocols allowed active on the network the more vulnerabilities there will be available to be exploited.
The SA will ensure the only network protocol used is TCP/IP all others are disabled.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD01.001: The reviewer will, with the assistance of the SA, verify that the only network protocol enabled is TCP/IP.

Fix(es): SPAN MFD01.001: Disable all protocols in the MFD except TCP/IP.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD01.002 CAT: **2** MFD or a printer is not using a static IP address

8500.2 IA Control:	DCBP-1	Category:	14.2 - Protocol Security
VMS Vul Key:	V0006778		

Vulnerability A MFD or a printer is not using a static IP address.

Vulnerability Discussion: Without static IP addresses, if the DNS cache is poisoned (corrupted) print files containing sensitive data could be redirected, leading to the compromise of sensitive data.
The SA will ensure all MFDs and printers are assigned a static IP.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD01.002: The reviewer will, with the assistance of the SA, verify that the MFD or printer is assigned a static IP address.

Fix(es): SPAN MFD01.002: Reconfigure the MFD or printer, assigning it a static IP address.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD01.003 CAT: 2 MFD/Printer Firewall/Router Rule Perimeter

8500.2 IA Control: DCBP-1 Category: 14.3 - Network Device Configuration

VMS Vul Key: V0006779

Vulnerability A firewall or router rule is not used to block all ingress and egress traffic from the enclave perimeter to the MFD or printer.

Vulnerability Discussion: Access to the MFD or printer from outside the enclave network could lead to a denial of service caused by a large number of large print files being sent to the device. Ability for the MFD or printer to access addresses outside the enclave network could lead to a compromise of sensitive data caused by forwarding a print file to a location outside of the enclave network. This is good defence in depth practice.
The SA will ensure there is a firewall or router rule to block all ingress and egress traffic from the enclave perimeter to the MFD or printer.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD01.003: The reviewer will interview the SA to verify that there is a firewall or router rule to block all ingress and egress traffic from the enclave perimeter to the MFD or printer.

Fix(es): SPAN MFD01.003: Ensure that there is a firewall or router rule to block all ingress and egress traffic from the enclave perimeter to the MFD or printer.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD02.001 CAT: 1 MFD SNMP Community Strings

8500.2 IA Control: IAIA-1: IAIA-2 Category: 14.2 - Protocol Security

VMS Vul Key: V0006781

Vulnerability The default passwords and SNMP community strings of all management services have not been replaced with complex passwords.

Vulnerability Discussion: There are many known vulnerabilities in the SNMP protocol and if the default community strings and passwords are not modified a unauthorized individual could gain control of the MFD or printer. This could lead to a denial of service or the compromise of sensitive data.
The SA will ensure the default passwords and SNMP community strings of all management services are replaced with complex passwords.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD02.001: The reviewer will, with assistance from SA, verify that the default passwords and SNMP community strings of all management services have not been replaced with complex passwords.

Fix(es): SPAN MFD02.001: Develop a plan to coordinate the modification of the default passwords and SNMP community strings of all management services replacing them with complex passwords. Obtain CM approval of the plan and execute the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD02.002 CAT: 1 MFD Configuration State After Power Down or Reboot

8500.2 IA Control: DCSS-1: DCSS-2 Category: 2.1 - Object Permissions

VMS Vul Key: V0006782

Vulnerability The MFD does not maintain its configuration state (passwords, service settings etc) after a power down or reboot.

Vulnerability Discussion: If the MFD does not maintain it state over a power down or reboot, it will expose the network to all of the vulnerabilities that where mitigated by the modifications made to its configuration state.
The SA will ensure the MFD maintains its configuration state (passwords, service settings etc) after a power down or reboot.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD02.002: Interview the SA and review the MFD documentation to verify that the MFD will maintain its configuration state (passwords, service settings etc) after a power down or reboot.

Fix(es): SPAN MFD02.002: Replace the MFD with a MFD that will maintain its configuration state (passwords, service settings etc) after a power down or reboot.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD02.003 CAT: 2 MFD Management Protocols

8500.2 IA Control: DCPP-1 Category: 14.4 - Unneeded Ports, Protocols, Hardware, and Services

VMS Vul Key: V0006783

Vulnerability All management protocols, with the exception of HTTPS and SNMPv3, are not disabled all times except when necessary to upgrade firmware or configure the device. Or, all other management services such as DHCP, SMTP, and BOOTP are not disabled at all times.

Vulnerability Discussion: Unneeded protocols expose the device and the network to unnecessary vulnerabilities.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD02.003: The reviewer will, with the assistance of the SA, verify that all management protocols, with the exception of HTTPS and SNMPv3, are not disabled all times except when necessary to upgrade firmware or configure the device. In addition, all other management services such as DHCP, SMTP, and BOOTP are disabled at all times.

Fix(es): SPAN MFD02.003: Disable all management protocols in accordance with the SPAN STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD02.004 CAT: 2 MFD Firmware

8500.2 IA Control: VIVM-1 Category: 3.2 - Operational / PM Patches

VMS Vul Key: V0006780

Vulnerability A MFD or a printer device is not flash upgradeable or is not configured to use the most current firmware available.

Vulnerability Discussion: MFD devices or printers utilizing old firmware can expose the network to known vulnerabilities leading to a denial of service or a compromise of sensitive data.
The SA will ensure devices are flash upgradeable and are configured to use the most current firmware available

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD02.004: The reviewer will, with the assistance of the SA, verify that the devices are flash upgradeable and are configured to use the most current firmware available.

Fix(es): SPAN MFD02.004: If the MFD or printer cannot be upgraded replace it.

If the MFD or printer can be upgraded but is not using the latest release of the firmware, upgrade the firmware.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD02.005 CAT: 1 MFD or a printer can be managed from any IP

8500.2 IA Control: DCBP-1 Category: 2.1 - Object Permissions

VMS Vul Key: V0006784

Vulnerability There is no restriction on where a MFD or a printer can be remotely managed.

Vulnerability Discussion: Since unrestricted access to the MFD or printer for management is not required the restricting the management interface to specific IP addresses decreases the exposure of the system to malicious actions. If the MFD or printer is compromised it could lead to a denial of service or a compromise of sensitive data.
The SA will ensure devices can only be remotely managed by SA’s or printer administrators from specific IPs (SA workstations and print spooler).

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD02.005: The reviewer will, with the assistance of the SA, verify that the MFD or printer can only be remotely managed by SA or printer administrator from specific IPs (SA workstations and print spooler). Look for list that restricts the protocol used for administrative access to specific IP addresses.

Fix(es): SPAN MFD02.005: Restrict access to the MFD's or printer's management function to a specific set of IP addresses. If the device lacks this functionality use an ACL in a router, firewall or switch to restrict the access.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD03.001 CAT: 3 Print Services Restricted to Port 9100 and/or LPD

8500.2 IA Control: DCBP-1 Category: 14.3 - Network Device Configuration

VMS Vul Key: V0006790

Vulnerability Print services for a MFD or printer are not restricted to Port 9100 and/or LPD (Port 515).

Where both Windows and non-Windows clients need services from the same device, both Port 9100 and LPD can be enabled simultaneously.

Vulnerability Discussion: Printer services running on ports other than the known ports for printing cannot be monitored on the network and could lead to a denial of service it the invalid port is blocked by a network administrator responding to an alert from the IDS for traffic on an unauthorized port.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD03.001: The reviewer will, with the assistance of the SA, verify that the MFD or printer print services are restricted to LPD or port 9100.

Where both Windows and non-Windows clients need services from the same device, both Port 9100 and LPD can be enabled simultaneously.

Fix(es): SPAN MFD03.001: Develop a plan to coordinate the reconfiguration of the printer servers and clients so that print services runs only on authorized ports. Obtain CM approval of the plan and implement the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD04.001 CAT: 2 MFD/Printer Restrict Jobs Only From Print Spooler

8500.2 IA Control: DCBP-1 Category: 2.1 - Object Permissions

VMS Vul Key: V0006794

Vulnerability A MFD or a printer is not configured to restrict jobs to those from print spoolers.

Vulnerability Discussion: If MFDs or printers are not restricted to only accepting print jobs from print spoolers that authenticate the user and log the job, a denial of service can be created by the MFD or printer accepting one or more large print jobs from an unauthorized user.
The SA will ensure MFDs and printers are configured to restrict jobs to only print spoolers, not directly from users.

The configuration is accomplished by restricting access, by IP, to those of the print spooler and SAs. If supported, IP restriction is accomplished on the device, or if not supported, by placing the device behind a firewall, switch or router with an appropriate discretionary access control list.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD04.001: The reviewer will, with the assistance of the SA, verify that MFDs and printers are configured to restrict jobs to only print spoolers, not directly from users.

The configuration is accomplished by restricting access, by IP, to those of the print spoolers and SAs. If supported, IP restriction is accomplished on the device or if not supported, by placing the device behind a firewall, switch or router with an appropriate discretionary access control list.

Fix(es): SPAN MFD04.001: Reconfigure the device to restrict access, by IP, to those of the print spoolers and SAs. If the device does not support this functionality, place the device behind a firewall, switch or router with an appropriate discretionary access control list.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD05.001 CAT: **2** MFD Authorized Users Restrictions

8500.2 IA Control: ECAN-1: IAIA-1: IAIA-2 Category: 2.1 - Object Permissions

VMS Vul Key: V0006796

Vulnerability Print spoolers are not configured to restrict access to authorized users and restrict users to managing their own individual jobs.

Vulnerability Discussion: If unauthorized users are allowed access to the print spooler they can queue large print file creating a denial of service for other users. If users are not restricted to manipulating only files they created, they could create ad denial of service by changing the print order of existing files or deleting other users files.
The SA will ensure print spoolers are configured to restrict access to authorized user and restrict users to managing their own individual jobs.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD05.001: The reviewer will, with the assistance of the SA, verify that the print spoolers are configured to restrict access to authorized users and restrict users to managing their own individual jobs.

Fix(es): SPAN MFD05.001: Configure the print spoolers to restrict access to authorized users and restrict users to managing their own individual jobs.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD06.001 CAT: **2** MFD and Spooler Auditing

8500.2 IA Control: ECAR-1: ECAR-2: ECAR-3 Category: 10.1 - Procedures

VMS Vul Key: V0006797

Vulnerability The devices and their spoolers do not have auditing enabled.

Vulnerability Discussion: Without auditing the identification and prosecution of an individual that performs malicious actions is difficult if not impossible.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD06.001: The reviewer will, with the assistance of the SA, verify that devices and their spoolers have auditing fully enabled.

Fix(es): SPAN MFD06.001: Configure the devices and their spoolers have auditing fully enabled.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD06.002 CAT: 3 MFD/Printer Security Policy

8500.2 IA Control: DCBP-1: ECAN-1: ECIC-1: IAIA-1: IAIA-2: PECS-1: PECS-2: PEDD-1   Category: 11.4 - Disposition

VMS Vul Key: V0006798

Vulnerability There is no security policy containing the requirements found in the SPAN STIG.

Acceptable use of device storage and retransmission of data (DODD 5200.1-R, Appendix G)
Verification that devices are not being shared on networks of different classification levels.
Procedures for scrubbing or disposing of hard disks when devices are sent out for repair or disposal.
Defined protocols for the maintenance, disposal, and purging of classified devices to include their non-volatile memory and storage devices.
Defined protocols for acceptable key operator codes, administration passwords, user codes, which personnel can change them, how often, format and storage of codes, and passwords.

Vulnerability Discussion: These policies are designed to raise the overall awareness of security practices and procedures. Failure to follow them can lead to the compromise of sensitive data.

The IAO will ensure implementation of a MFD and printer security policy to include:

Acceptable use of device storage and retransmission of data (DODD 5200.1-R, Appendix G)
Verification that devices are not being shared on networks of different classification levels.
Procedures for scrubbing or disposing of hard disks when devices are sent out for repair or disposal.
Defined protocols for the maintenance, disposal, and purging of classified devices to include their non-volatile memory and storage devices.
Defined protocols for acceptable key operator codes, administration passwords, user codes, which personnel can change them, how often, format and storage of codes, and passwords.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD06.002: Interview the IAO to verify that there is a security policy that meets the requirements of the SPAN STIG implemented.

Fix(es): SPAN MFD06.002: Implement a MFD and printer security policy in accordance with the SPAN STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD06.006 CAT: 3 MFD Level of Audit and Reviewing

8500.2 IA Control: ECAR-1: ECAR-2: ECAR-3: ECAT-1: ECAT-2 Category: 10.2 - Content Configuration

VMS Vul Key: V0006799

Vulnerability The level of audit has not been established by the IAO or the audits logs being collected for the devices and print spoolers are not being reviewed.

Vulnerability Discussion: If inadequate information is captured in the audit, the identification and prosecution of malicious user will be very difficult. If the audits are not regularly reviewed suspicious activity may go undetected for a long time.
The IAO will define a level of auditing to perform to include who reviews the audit logs.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD06.006: The reviewer will interview the IAO to verify that the level of auditing has been established and that audit logs are being reviewed.

Auditing will include user, key operator and admin codes and passwords, enabled features and services. Any deviation from the baseline should be treated as a potential security incident. Ensure operational security controls are in place to ensure servicing of devices by authorized personnel is in accordance with change and configuration protocols.

Fix(es): SPAN MFD06.006: Implement a level of auditing in accordance with the requirements in the SPAN STIG and establish a procedure to ensure regular review or the audit logs.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD07.001 CAT: 1 MFD Classified Network

8500.2 IA Control: DCBP-1 Category: 9.1 - SABI

VMS Vul Key: V0006800

Vulnerability MFDs with copy, scan, or fax capability are allowed on classified networks without the approved of the DAA.

Vulnerability Discussion: MFDs with copy, scan, or fax capabilities if compromised could lead to the compromise of classified data or the compromise of the network.
The IAO will ensure MFDs with copy, scan, or fax capability are not allowed on classified networks unless approved by the DAA.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD07.001: The reviewer will interview the IAO to verify that MFDs with copy, scan or fax capabilities are not allowed on classified networks unless approved by the DAA.

Fix(es): SPAN MFD07.001: Remove the MFD from the classified network or obtain DAA approval.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD07.002 CAT: 2 MFD Clearing Disk Space Scan to Disk

8500.2 IA Control: ECRC-1 Category: 11.4 - Disposition

VMS Vul Key: V0006801

Vulnerability A MFD device, with scan to hard disk functionality used, is not configured to clear the hard disk between jobs.

Vulnerability Discussion: If the MFD is compromised the un-cleared, previously used, space on the hard disk drive can be read which can lead to a compromise of sensitive data.
The SA will ensure the device is configured to clear the hard disk between jobs if scan to hard disk functionality is used.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD07.002: The reviewer, with the assistance of the SA, verify the device is configured to clear the hard disk between jobs if scan to hard disk functionality is used.

Fix(es): SPAN MFD07.002: Configured the MFD to clear the hard disk between jobs if scan to hard disk functionality is used.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD07.003 CAT: 3 MFD Scan Discretionary Access Control

8500.2 IA Control: ECAN-1 Category: 2.1 - Object Permissions

VMS Vul Key: V0006802

Vulnerability Scan to a file share is enabled but the file shares do not have the appropriate discretionary access control list in place.

Vulnerability Discussion: Without appropriate discretionary access controls unauthorized individuals may read the scanned data. This can lead to a compromise of sensitive data.
The SA will ensure file shares have the appropriate discretionary access control list in place if scan to a file share is enabled.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD07.003: The reviewer will, with the assistance of the SA, verify that file shares have the appropriate discretionary access control list in place if scan to a file share is enabled.

Fix(es): SPAN MFD07.003: Create the appropriate discretionary access control list for file shares if scan to a file share is enabled.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD07.004 CAT: **3** MFD Fax from Network Auditing

8500.2 IA Control: ECAR-1: ECAR-2: ECAR-3 Category: 10.2 - Content Configuration

VMS Vul Key: V0006803

Vulnerability Fax from the network is enabled but auditing of user access and fax log is not enabled.

Vulnerability Discussion: Without auditing the originator and destination of a fax cannot be determined. Prosecuting of an individual who maliciously compromises sensitive data via a fax will be hindered without audits.
The SA will ensure auditing of user access and fax log is enabled if fax from the network is enabled.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD07.004: The reviewer will, with the assistance of the SA, verify that auditing of user access and fax log is enabled if fax from the network is enabled.

Fix(es): SPAN MFD07.004: Configure the MFD to audit faxing in accordance with the SPAN STIG. If this is not possible, disable the fax functionality and disconnect the phone line from the MFD.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD07.005 CAT: **2** MFD Scan to SMTP (email)

8500.2 IA Control: DCBP-1 Category: 14.4 - Unneeded Ports, Protocols, Hardware, and Services

VMS Vul Key: V0006804

Vulnerability Devices allow scan to SMTP (email).

Vulnerability Discussion: The SMTP engines found on the MFDs reviewed when writing the SPAN STIG did not have robust enough security features supporting scan to email. Because of the lack of robust security scan to email will be disabled on MFD devices. Failure to disable this feature could lead to an untraceable and possibly undetectable compromise of sensitive data.
The SA will ensure devices do not allow scan to SMTP.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD07.005: The reviewer will, with the assistance of the SA, verify that devices do not allow scan to SMTP.

Fix(es): SPAN MFD07.005: Disable the scan to SMTP (email) feature on all MFDs.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD08.001 CAT: 2 MFD Hard Drive Lock

8500.2 IA Control: PECF-1: PECF-2 Category: 5.9 - Device Locations

VMS Vul Key: V0006805

Vulnerability A MFD device does not have a mechanism to lock and prevent access to the hard drive.

Vulnerability Discussion: If the hard disk drive of a MFD can be removed from the MFD the data on the drive can be recovered and read. This can lead to a compromise of sensitive data.

The IAO will ensure the device has a mechanism to lock and prevent access to the hard disk.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD08.001: The reviewer will, with the assistance of the SA, verify that the device has a mechanism to lock and prevent access to the hard disk.

What we are looking for here is a locking mechanism with a key securing the hard drive or the case access to the hard drive. The lock will be locked or this is a finding.

Fix(es): SPAN MFD08.001: If the lock is not locked, lock it.

If there is no lock see if the vendor makes one and if so acquire it an lock the drive.
If the vendor does not supply a lock, acquire an aftermarket lock that will secure the drive so that it cannot be accessed. Even a drive that cannot be removed but the connectors can be removed is vulnerable.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

MFD08.002 CAT: 1 MFD/Printer Global Configuration Settings

8500.2 IA Control: ECAN-1 Category: 2.1 - Object Permissions

VMS Vul Key: V0006806

Vulnerability The device is not configured to prevent non-printer administrators from altering the global configuration of the device.

Vulnerability Discussion: If unauthorized users can alter the global configuration of the MFD they can remove all security. This can lead to the compromise of sensitive data or the compromise of the network the MFD is attached to.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN MFD08.002: The reviewer will, with the assistance of the SA, verify that the device is configured to prevent non-printer administrators from altering the global configuration of the device.

Fix(es): SPAN MFD08.002: Configured the device to prevent non-printer administrators from altering the global configuration of the device. If the device cannot be configured in this manner, replace the device with one that can be configured in an acceptable manner.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes: